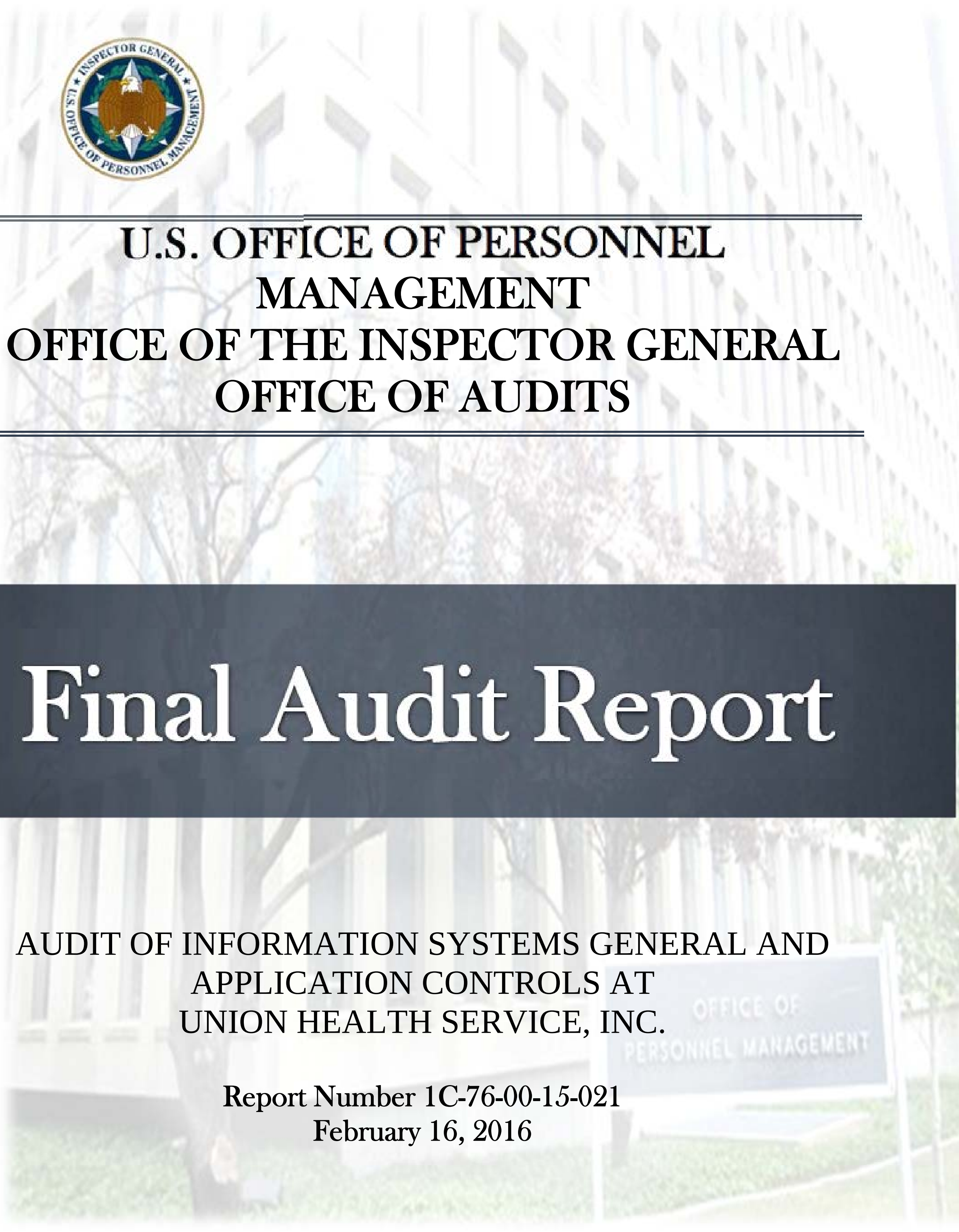

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

AUDIT OF INFORMATION SYSTEMS GENERAL AND APPLICATION CONTROLS AT UNION HEALTH SERVICE, INC.

Report Number 1C-76-00-15-021
February 16, 2016

-- CAUTION --

This audit report has been distributed to Federal officials who are responsible for the administration of the audited program. This audit report may contain proprietary data which is protected by Federal law (18 U.S.C. 1905). Therefore, while this audit report is available under the Freedom of Information Act and made available to the public on the OIG webpage (*http://www.opm.gov/our-inspector-general*), caution needs to be exercised before releasing the report to the general public as it may contain proprietary information that was redacted from the publicly distributed copy.

EXECUTIVE SUMMARY

Audit of Information Systems General and Application Controls at Union Health Service, Inc.

Report No 1C-76-00-15-021 **February 16, 2016**

Background

Union Health Service, Inc. (UHS) contracts with the U.S. Office of Personnel Management (OPM) as part of the Federal Employees Health Benefits Program (FEHBP).

Why Did We Conduct the Audit?

The objectives of this audit were to evaluate controls over the confidentiality, integrity, and availability of Federal Employee Health Benefit Plan data processed and maintained in UHS's information technology (IT) environment.

What Did We Audit?

The scope of this audit centered on the information systems used by UHS to process encounters and medical insurance claims for FEHBP members, and included all systems that process or store federal data.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

This audit report contains a large number of recommendations to improve the IT security posture of UHS. However, we would like to note that we believe that UHS takes its cybersecurity program seriously and is putting forth its best effort to secure the sensitive Federal data it processes. UHS is a relatively small organization, and it has already implemented a wide variety of IT security controls using the very limited IT resources it has. Some of the opportunities for improvement that we noted include:

- UHS's security management program could be improved.
- UHS could improve its logical and physical access controls in the following areas:
  - Information system authentication requirements;
  - User activity monitoring;
  - Logical access review; and
  - Data center physical access.
- We noted several concerns with UHS's network security controls:
  - UHS's network architecture does not segregate sensitive data and applications from the rest of the environment;
  - UHS does not have the capability to monitor for suspicious activity within its network;
  - UHS does not have documented procedures for identifying, reporting, and handling network security incidents; and
  - UHS does perform external vulnerability scans annually, however it does not conduct routine full-scope vulnerability scanning on its internal network.
- UHS does not have documented baseline configurations for its computer servers, and therefore it is not possible to routinely audit the actual settings of a computer server against the approved configuration settings. We also noted that UHS does not test software patches before they are deployed to the production environment.

EXECUTIVE SUMMARY

Audit of Information Systems General and Application Controls at Union Health Service, Inc.

- With regards to contingency planning we noted that:
  - UHS has not conducted an adequate business impact analysis that identifies and prioritizes critical information systems;
  - UHS has not established an alternate/backup facility to recover its IT operations in the event of a disaster or documented the steps necessary to resume operations;
  - Environmental controls at UHS's data center could be improved with the implementation of a fire suppression system;
  - UHS does not perform contingency plan testing to evaluate the effectiveness of the plan and the organizational readiness to execute the plan;
  - UHS does not perform periodic emergency response training to reinforce the activities that personnel will need to perform in an emergency situation; and
  - UHS does not use [redacted] for its backup tapes that are transferred offsite weekly.

- UHS has implemented multiple controls over its member encounter and claims adjudication processes to ensure that FEHBP encounters and claims are processed accurately. However, we observed that paper claims containing sensitive information are stored in an unlocked file cabinet within the UHS facility.

ABBREVIATIONS

BIA	**Business Impact Analysis**
CFR	**Code of Federal Regulations**
FEHBP	**Federal Employees Health Benefits Program**
FISCAM	**Federal Information System Controls Audit Manual**
GAO	**U.S. Government Accountability Office**
HIO	**Healthcare and Insurance Office**
IDS	**Intrusion Detection System**
IT	**Information Technology**
NIST	**National Institute of Standards and Technology**
OIG	**Office of the Inspector General**
OMB	**U.S. Office of Management and Budget**
OPM	**U.S. Office of Personnel Management**
PHI	**Protected Health Information**
SDLC	**System Development Life Cycle**
SP	**Special Publication**
UHS	**Union Health Service, Inc.**

TABLE OF CONTENTS

Page

EXECUTIVE SUMMARY i

ABBREVIATIONS iii

I. **BACKGROUND** 1

II. **OBJECTIVES, SCOPE, AND METHODOLOGY** 2

III. **AUDIT FINDINGS AND RECOMMENDATIONS** 4
A. Security Management 4
B. Access Controls 5
C. Network Security 10
D. Configuration Management 16
E. Contingency Planning 18
F. Application Controls 25

IV. **MAJOR CONTRIBUTORS TO THIS REPORT** 28

APPENDIX: Union Health Service's November 2, 2015 response to the draft audit report, issued September 1, 2015.

REPORT FRAUD, WASTE, AND MISMANAGEMENT

I. BACKGROUND

This final report details the findings, conclusions, and recommendations resulting from the audit of general and application controls over the information systems responsible for processing Federal Employees Health Benefits Program (FEHBP) data by Union Health Service, Inc. (UHS).

The audit was conducted pursuant to FEHBP contract CS 1571; 5 U.S.C. Chapter 89; and 5 Code of Federal Regulations (CFR) Chapter 1, Part 890. The audit was performed by the U.S. Office of Personnel Management's (OPM) Office of the Inspector General (OIG), as established by the Inspector General Act of 1978, as amended.

The FEHBP was established by the Federal Employees Health Benefits Act, enacted on September 28, 1959. The FEHBP was created to provide health insurance benefits for federal employees, annuitants, and qualified dependents. The provisions of the Act are implemented by OPM through regulations codified in Title 5, Chapter 1, Part 890 of the CFR. Health insurance coverage is made available through contracts with various carriers that provide service benefits, indemnity benefits, or comprehensive medical services.

This was our first audit of UHS's information technology (IT) general and application controls. UHS is a small organization and although this report details many areas where controls could be improved in comparison to industry standards, UHS has already implemented a notable number of controls considering the limited resources and personnel available. All UHS personnel that worked with the auditors were helpful and open to ideas and suggestions. They viewed the audit as an opportunity to examine practices and to make changes or improvements as necessary. Their positive attitude and helpfulness throughout the audit was greatly appreciated.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

The objectives of this audit were to evaluate controls over the confidentiality, integrity, and availability of FEHBP data processed and maintained in UHS's IT environments. We accomplished these objectives by reviewing the following areas:

- Security management;
- Access controls;
- Network Security;
- Configuration management;
- Segregation management;
- Contingency planning; and
- Application controls specific to UHS's member encounter process.

Scope and Methodology

This performance audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States. Accordingly, we obtained an understanding of UHS's internal controls through interviews and observations, as well as inspection of various documents, including information technology and other related organizational policies and procedures. This understanding of UHS's internal controls was used in planning the audit by determining the extent of compliance testing and other auditing procedures necessary to verify that the internal controls were properly designed, placed in operation, and effective.

The scope of this audit centered on the information systems used by UHS to process and/or store the data of FEHBP members. The business processes reviewed are primarily located in Chicago, Illinois.

The onsite portion of this audit was performed in April, 2015. We completed additional audit work before and after the on-site visit at our office in Washington, D.C. The findings, recommendations, and conclusions outlined in this report are based on the status of information system general and application controls in place at UHS as of May, 2015.

In conducting our audit, we relied to varying degrees on computer-generated data provided by UHS. Due to time constraints, we did not verify the reliability of the data used to complete some of our audit steps, but we determined that it was adequate to achieve our audit objectives. However, when our objective was to assess computer-generated data, we completed audit steps necessary to obtain evidence that the data was valid and reliable.

In conducting this review we:

- Gathered documentation and conducted interviews;
- Reviewed UHS's business structure and environment;
- Performed a risk assessment of UHS's information systems environment and applications, and prepared an audit program based on the assessment and the U.S. Government Accountability Office's (GAO) Federal Information System Controls Audit Manual (FISCAM); and
- Conducted various compliance tests to determine the extent to which established controls and procedures are functioning as intended. As appropriate, we used judgmental sampling in completing our compliance testing.

Various laws, regulations, and industry standards were used as a guide to evaluating UHS's control structure. These criteria include, but are not limited to, the following publications:

- Title 48 of the Code of Federal Regulations;
- U.S. Office of Management and Budget (OMB) Circular A-130, Appendix III;
- OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information;
- Information Technology Governance Institute's CobiT: Control Objectives for Information and Related Technology;
- GAO's FISCAM;
- National Institute of Standards and Technology's Special Publication (NIST SP) 800-12, Introduction to Computer Security;
- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems;
- NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments;
- NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems;
- NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy;
- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations;
- NIST SP 800-61, Revision 2, Computer Security Incident Handling Guide;

Compliance with Laws and Regulations

In conducting the audit, we performed tests to determine whether UHS's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, UHS was not in complete compliance with all standards, as described in section III of this report.

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. Security Management

UHS does not perform routine risk assessments.

The security management component of this audit involved the examination of the policies and procedures that are the foundation of UHS's overall IT security program. We evaluated UHS's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

UHS has implemented a series of formal policies and procedures that comprise its security management program. UHS also maintains adequate policies and procedures related to risk management. However, UHS does not perform formal risk assessments on a routine basis.

According to NIST SP 800-53, Revision 4, the organization should conduct "an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits …." Furthermore, the organization should document risk assessment results, review risk assessment results, disseminate risk assessment results and update the risk assessment.

Additionally, NIST SP 800-30, Revision 1, states, "Risk assessment is the first process in the risk management methodology. Organizations use risk assessment to determine the extent of the potential threat and the risk associated with an IT system throughout its SDLC."

Failure to conduct periodic risk assessments inhibits UHS's ability to secure the IT systems that store and process proprietary and confidential information, as a thorough risk assessment process would enable UHS to make well-informed risk management decisions.

We also reviewed UHS's human resources policies and procedures related to hiring, training, transferring, and terminating employees. Nothing came to our attention to indicate that UHS does not have adequate human resource policies and procedures.

Recommendation 1

We recommend that UHS implement a process to perform routine risk assessments that includes formal documentation and a periodic review of the risk assessment.

Plan Response:

"After review we agree that a more formal risk assessment process should be implemented, along with formal documentation and a periodic review of the risk assessment. See Risk Assessment Policy document attached."

OIG Comment:

The evidence provided by UHS in response to the draft audit report indicates that the Plan is actively working to develop policies related to risk assessments. However, the recommendation should remain open until a formal risk assessment has been performed in accordance with the new policy. As part of the audit resolution process, UHS should provide OPM's Healthcare and Insurance Office (HIO) with evidence that this recommendation has been addressed. This statement also applies to all subsequent recommendations in this report that UHS agrees to implement.

B. Access Controls

Access controls are the policies, procedures, and techniques used to prevent or detect unauthorized physical or logical access to sensitive resources.

We examined the physical access controls of UHS's facilities and data centers. We also examined the logical controls protecting sensitive data on UHS's network environment and claims processing-related applications.

The access controls observed during this audit include, but are not limited to:

- Procedures for appropriately granting and removing physical access to the facility and data center; and
- Procedures for authorizing and revoking logical access to applications.

The following section documents several opportunities for improvement related to UHS's access controls.

1. Authentication Requirements

UHS has documented organization-wide information system authentication standards. However, we determined that several of the standards are weaker than the controls that we typically observe at similar organizations. We also discovered instances where UHS's information systems were not configured in compliance with the corporate standards.

The “Access Controls” section of FISCAM provides guidance for implementing strong authentication controls.

Failure to enforce strong authentication requirements on information systems increases the risk that the systems could be breached by brute force password attacks.

Recommendation 2

We recommend that UHS strengthen its authentication requirements to better align with industry best practices.

Plan Response:

“Network and EMR passwords have been implemented to meet a more stringent authentication requirement.”

OIG Comment:

The evidence provided by UHS in response to the draft audit report indicates that the Plan has improved their authentication requirements policy to better align with industry best practices; no further action is required.

Recommendation 3

We recommend that UHS make the appropriate system changes to ensure that all of its information systems are configured in compliance with the approved authentication requirements.

Plan Response:

“Network and EMR passwords have been implemented to meet a more stringent authentication requirement.”

OIG Comment:

Evidence provided by UHS in response to the draft audit report indicates that the Plan has improved its authentication standards to better align with industry best practice. However, no evidence has been provided to indicate that the new authentication requirements have been implemented/enforced on the information systems. As part of the audit resolution process, UHS should provide OPM’s HIO with evidence that the authentication settings required by the policy have been implemented on all major systems and applications that require unique authentication.

2. Privileged User Authentication

Privileged users (system administrators) of UHS's information systems have more stringent authentication requirements than regular users. While this is a good control, UHS's management of privileged user accounts could be improved with [redacted].

[redacted]

Recommendation 4

We recommend that UHS implement [redacted] for privileged user access to all information systems

Plan Response:

"Privileged user authentication will be evaluated for implementation next year. Consideration on network impact, budget and workflow will be paramount in the decision factor."

3. User Activity Monitoring

Monitoring user access to information systems is a critical component to an organization's security assurance process for information systems. UHS currently does not monitor access for general employees or, more importantly, it does not monitor information system access or activity for privileged users.

NIST SP 800-53, Revision 4, states the organization should monitor the user of information system accounts and monitor privileged role assignments and activities.

Failure to monitor general user and privileged user access increases the risk of an insider attack against the organization.

<u>Recommendation 5</u>

We recommend that UHS implement procedures for monitoring user activity. Monitoring of log-on and log-off activity should be monitored for all users. In addition, the actual activity of privileged users (i.e., transactions performed from these accounts) should be logged and monitored.

<u>Plan Response:</u>

"We researched and tested [redacted] active directory monitoring tool. This program provides significant logs that allow users to be monitored in relation to access to our systems. This software [was installed on September 30th, 2015] and is fully functional on all servers."

<u>OIG Comment:</u>

The evidence provided by UHS in response to the draft audit report indicates that the Plan has implemented procedures for monitoring user activity; no further action is required.

4. Access Review

UHS does not have a process in place to routinely review user accounts to ensure that they only have access to the data and applications required to perform their job function.

NIST SP 800-12, An Introduction to Computer Security, states that "it is necessary to review user account management on a system." Access reviews should "examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up-to-date, whether required training has been completed, and so forth."

Failure to routinely audit active user accounts for appropriateness increases the risk that individuals have unapproved and/or unnecessary access to sensitive and proprietary information.

<u>Recommendation 6</u>

We recommend that UHS implement a process to routinely audit the privileges of all active network and application user accounts for appropriateness.

Plan Response:

"We researched and tested [redacted] active directory monitoring tool. This program provides significant logs that allow users to be monitored in relation to access to our systems. This software [was installed on September 30th, 2015] and is fully functional on all servers."

OIG Comment:

No evidence has been provided to indicate that UHS has a process in place to review active user accounts for appropriateness. The implementation of [redacted] addresses recommendation 5 (see above), monitoring user activity. However, we would like to see evidence that a routine review is conducted in order to confirm that active user(s) still require access and that the type of access is appropriate for the their job function.

5. Data Center Physical Access

UHS is in the process of moving its production technical environment to a third party data center with satisfactory physical and environmental controls. However, the current data center, which will later be used as a backup location, did not contain several controls that we typically observe at similar facilities, including:

- [redacted]; and
- [redacted].

[redacted]

Failure to implement proper physical access controls increases the risk that unauthorized individuals can gain access to UHS's data center and the sensitive resources and confidential data it contains.

NIST SP 800-53, Revision 4, provides guidance for adequately controlling physical access to information systems containing sensitive data.

<u>Recommendation 7</u>

We recommend that UHS improve the physical access controls of its data center. At a minimum, the computer room should have [redacted] and [redacted] controls.

<u>Plan Response:</u>

"We have implemented [redacted] ***for our server room access."***

<u>OIG Comment:</u>

Evidence provided by UHS in response to the draft audit report indicates that the Plan has implemented [redacted] to gain access to its data center. However, this only addresses part of the recommendation. We would also like to see evidence that [redacted] controls have been implemented.

As part of the audit resolution process, UHS should provide OPM's HIO with evidence that it has adequately implemented this recommendation.

C. <u>Network Security</u>

Network security includes the policies and controls used to prevent or monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

We evaluated UHS's network security program and reviewed the results of several automated vulnerability scans that we performed during this audit. We noted the following opportunities for improvement related to UHS's network security controls.

1. Network Segmentation

UHS uses a perimeter firewall to control connections with systems outside of its network. However, no segmentation of the internal network has been implemented in order to segregate systems that have different security requirements. Of primary concern, we observed that there is no separation between the public facing web server and sensitive internal database and application servers.

NIST SP 800-53, Revision 4, requires an organization to implement subnetworks for publicly accessible system components that are separated from internal organizational networks. NIST SP 800-41, Revision 1, also states that organizations should use firewalls "where security requirements vary among their internal networks."

Failure to securely separate technical resources increases the risk that a compromise of a publicly accessible system could also allow access to internal assets and data.

Recommendation 8

We recommend that UHS segregate its network with subnetworks in order to physically and/or logically separate (communication occurring only through managed interfaces) sensitive resources from public facing web servers.

Plan Response:

"We do agree to segregate our network with sub networks. Because of the cost and infrastructure impact we have scheduled this project Implementation for [redacted]***."***

2. Network Monitoring

The UHS network has an intrusion detection system (IDS) built into the firewalls that is capable of monitoring suspicious activity. However, since the network is not segmented and there are not any IDS sensors placed on the internal network, there is no capacity to monitor for suspicious activity within the network. Additionally, UHS does not routinely review the IDS and network device logs currently produced.

NIST SP 800-53, Revision 4, states that organizations should monitor and control communications at the external boundary of the system and at key internal boundaries within the system.

NIST SP 800-53, Revision 4, also states that organizations should routinely review and analyze information system audit records for indications of inappropriate or unusual activity. Failure to routinely review suspicious network event logs and alerts could allow an intrusion to go undetected.

Recommendation 9

We recommend that UHS implement additional network event monitoring capabilities and implement a process to routinely review audit records for suspicious activity.

Plan Response:

"We have implemented [redacted] ***monitoring tool."***

OIG Comment:

Evidence provided by UHS in response to the draft audit report indicates that the Plan has implemented a tool to monitor network events. However, we would also like to see evidence that a process to routinely review audit records gathered by the tool is carried out. As part of the audit resolution process, UHS should provide OPM's HIO with evidence that it has fully implemented this recommendation.

3. Incident Response Procedures

UHS has an incident response policy that conveys the need for an incident response program with documented procedures. However, procedures for identifying, reporting, and handling incidents have not been developed. A typical incident response program would identify a formal incident response team, design detection and response capabilities, and periodically test the effectiveness of the plan.

UHS does not have formal incident response procedures.

FISCAM states, "It is important that an entity have formal written procedures for reporting security violations or suspected violations to a central security management office so that multiple related incidents can be identified, other employees can be alerted to potential threats, and appropriate investigations can be performed."

NIST SP 800-53, Revision 4, requires that the organization "Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery[.]" FISCAM also states that "Without prompt and appropriate responses to security incidents, violations could continue to occur and cause damage to an entity's resources indefinitely."

Recommendation 10

We recommend that UHS develop and implement incident response procedures in accordance with NIST SP 800-53, Revision 4.

Plan Response:

"We are reviewing your suggested article and will continue [to] implement suggested procedures that fit our infrastructure."

4. Full Scope Vulnerability Scanning

We conducted a review of UHS's computer server vulnerability management program to determine if adequate controls were in place to detect, track, and remediate vulnerabilities.

UHS performs scans on its externally accessible servers once per year to detect vulnerabilities. However, scans are not conducted on internal systems such as servers, databases, applications, network devices, and workstations. We also found that UHS does not have a formal process for tracking and remediating vulnerabilities detected in the external scans.

NIST SP 800-53, Revision 4, states that the organization should scan "for vulnerabilities in the information system and hosted applications . . . ."

FISCAM states that "When weaknesses are identified, the related risks should be reassessed, appropriate corrective or remediation actions taken, and follow-up monitoring performed to make certain that corrective actions are effective."

Failure to perform full scope vulnerability scanning increases the risk that vulnerabilities in UHS's systems remain unidentified, increasing the risk of a system breach.

Recommendation 11

We recommend that UHS implement a process to routinely conduct vulnerability scanning on the entire network environment and to formally track and remediate vulnerabilities detected during scans in a timely manner.

Plan Response:

"IT network support staff will perform a vulnerability scan every 6 months. Document and remediate all critical vulnerabilities. If there is no apparent fix; propose a procedure using firewalls and limited access plus constant scanning."

OIG Comment:

Evidence provided by UHS in response to the draft audit report indicates that the Plan has implemented an adequate policy and procedure related to vulnerability scanning and vulnerability remediation. As part of the audit resolution process, UHS should provide OPM's HIO with evidence that routine vulnerability scans have been conducted in accordance with the Plan's policy.

5. Vulnerabilities Identified in Scans

System Patching

UHS has not documented formal patch management policies and procedures. The results of our vulnerability scans indicate that a majority of the servers tested are missing critical patches, service packs, and hot fixes that are not being implemented in a timely manner.

FISCAM states that "Software should be scanned and updated frequently to guard against known vulnerabilities." NIST SP 800-53, Revision 4, states that the Plan must identify, report, and correct information system flaws and install security-relevant software and firmware updates promptly.

Failure to promptly install important updates increases the risk that known vulnerabilities exist on information systems.

Recommendation 12

We recommend that UHS implement policies and procedures to ensure that all computer servers are updated with appropriate patches, service packs, and hotfixes on a timely basis.

Plan Response:

"We have removed all non-current and non-supported software from servers. We check all software monthly for critical patches and upgrades [a]fter review[ing] appropriate and critical software[.] See IT Risk Assessment Policy"

OIG Comment:

Evidence provided by UHS in response to the draft audit report indicates that the Plan has implemented an adequate policy and procedure related to vulnerability scanning, patching, and vulnerability remediation; no further action is required.

Noncurrent Software

The results of the vulnerability scans also indicated that several servers contained noncurrent software applications that were no longer supported by the vendors, and have known security vulnerabilities.

FISCAM states that "Procedures should ensure that only current software releases are installed in information systems. Noncurrent software may be vulnerable to malicious code such as viruses and worms." Failure to promptly remove outdated software increases the risk of a successful malicious attack on the information system.

Recommendation 13

We recommend that UHS implement a process to ensure only current and supported versions of software applications are installed on the production servers. This should include a process for documenting known instances where unsupported software is required for business reasons.

Plan Response:

"We have removed all non-current and non-supported software from servers. We check all software monthly for critical patches and upgrades [a]fter review[ing] appropriate and critical software[.] See: IT Risk Assessment Policy"

OIG Comment:

As part of the audit resolution process, UHS should provide OPM's HIO with evidence (copies of its own vulnerability scans) that indicates that unsupported software has been removed from its environment. UHS should also provide formal documentation justifying any instances of unsupported software required for business reasons.

Insecure Operating System Configuration

The results of the vulnerability scans also indicated that several UHS servers contained insecure configurations that could allow hackers or unprivileged users unauthorized access to sensitive and proprietary information.

NIST SP 800-53, Revision 4, states that the Plan must scan for vulnerabilities in the information system and hosted applications, analyze the reports, and remediate legitimate vulnerabilities. Failure to remediate vulnerabilities increases the risk that hackers could exploit system weaknesses for malicious purposes.

Recommendation 14

We recommend that UHS remediate the specific technical weaknesses outlined in the vulnerability scanning audit inquiry issued during the audit.

Plan Response:

"We have taken action to remediate the specific technical weakness outlined by applying all patches and hotfixes required on servers. We have also secured our internet and intranet servers by applying* [redacted]*."

OIG Comment:

Evidence provided by UHS in response to the draft audit report indicates that the Plan has implemented an adequate policy and procedure related to vulnerability scanning, patching, and vulnerability remediation. As part of the audit resolution process, UHS should provide OPM's HIO with copies of its own vulnerability scans that demonstrate that the technical weaknesses discovered during this audit have been remediated.

D. Configuration Management

We evaluated UHS's management of the configuration of its servers and databases supporting the claims adjudication system.

The sections below document areas for improvement related to UHS's configuration management controls.

1. Baseline Configurations

UHS has not documented formal baseline configurations for its computer servers. A baseline configuration is a formally approved standard outlining how to securely configure a specific operating platform.

NIST SP 800-53, Revision 4, requires an organization to develop a configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, as well as procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

In addition, NIST SP 800-53, Revision 4, states that an organization must develop, document, and maintain a current baseline configuration of the information system.

Failure to establish approved system configuration settings increases the risk the system may not be configured in a secure manner.

Recommendation 15

We recommend that UHS document approved baseline configurations for all operating platforms and databases that it uses in its technical environment.

Plan Response:

"See baseline server configuration documentation[.]"

OIG Comment:

The documentation provided by UHS in response to the draft audit report does not fully address the recommendation. A comprehensive baseline server configuration documentation should address a variety of settings such as account lockout policy, password policy, audit policy, event logs, user rights, etc. NIST Special Publication 800-53, Revision 4, control CM-2 provides guidance on baseline configurations.

As part of the audit resolution process, UHS should provide OPM's HIO with evidence that adequate baseline configurations have been approved and documented by the Plan.

2. Configuration Compliance Auditing

As noted above, UHS does not maintain approved baseline configurations, and therefore cannot effectively audit its system security settings (i.e., there are no approved settings to which to compare the actual settings).

NIST SP 800-53, Revision 4, states that an organization must monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

FISCAM requires current configuration information to be routinely monitored for accuracy. Monitoring should address the baseline and operational configuration of the hardware, software, and firmware that comprise the information system.

Failure to implement a thorough configuration compliance auditing program increases the risk that insecurely configured servers exist undetected, creating a potential gateway for malicious virus and hacking activity that could lead to data breaches.

Recommendation 16

We recommend that UHS implement a process to routinely audit security configuration settings to ensure they are in compliance with the approved configuration baselines.

Plan Response:

"To assure that our network servers' security configurations are in compliance, we will check all servers quarterly."

3. Patching Procedures

When UHS installs security patches on its computer servers, these patches are installed directly onto production servers without being tested. Failure to test patches before implementing them in the production environment increases the risk that an application will not function as intended due to an unforeseen side effect of the patch.

NIST 800-53, Revision 4, states that the organization should test "software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation[.]"

Recommendation 17

We recommend that UHS test all patches prior to implementation in the production environment.

Plan Response:

"Standard application operating Patches are always tested in test environments for critical application. Before applying patches to production a snap shot is taken. Snap shots are used for application restore in case of an issue. Other patches are applied based on industry standards."

OIG Comment:

During the audit we were informed that security patches are pushed to production without any testing. As part of the audit resolution process, UHS should provide OPM's HIO with evidence that security patches are tested before being released to the production environment.

E. Contingency Planning

We reviewed UHS's contingency planning program to determine whether controls are in place to prevent or minimize interruptions to business operations when disastrous events occur. We determined that UHS has documented procedures to support business operations and IT system continuity during such disruptions. However, we identified the following opportunities for improvement related to UHS's contingency planning program.

1. Business Impact Analysis

UHS has not conducted an adequate business impact analysis (BIA). We were provided with an operations recovery plan that maps possible interruption scenarios to the potential business areas affected and the corresponding contingency plan section that would be followed if that event occurred. However, this BIA does not contain several of the requirements documented in NIST 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems. Specifically, the BIA did not identify and prioritize critical IT systems.

NIST 800-34, Revision 1, states that, "the BIA is a key step in implementing . . . the contingency planning process." Three steps involved in accomplishing a BIA include determining business processes and recovery criticality, identifying resource requirements, and identifying recovery priorities for system resources.

Failure to conduct a BIA increases the risk that UHS will not be able to recover critical business operations in a timely manner.

Recommendation 18

We recommend that UHS conduct a business impact analysis in accordance with NIST 800-34, Revision 1. Specifically, UHS should identify and prioritize critical IT systems and components and use this information to determine contingency requirements and priorities.

Plan Response:

"We feel that [our] Business Continuity plan already takes this into consideration. However we are reviewing your NIST 800-34 to identify and implement relevant information."

OIG Comment:

Key elements missing in UHS's BIA include the identification of recovery criticality, resource requirements, and recovery priorities. As part of the audit resolution process, UHS should provide OPM's HIO with evidence that it has conducted a BIA that addresses the requirements of NIST SP 800-34, Revision 1.

2. Contingency Plan

UHS does not have an adequate contingency plan.

UHS's contingency plan does not address some of the suggested elements of NIST SP 800-34, Revision 1. UHS has developed an operations recovery plan as well as an IT disaster recovery plan. However, these plans do not include specific requirements and steps to follow for the recovery phase of contingency operations. The sequence of activities should reflect system priorities identified in the BIA, and should provide detailed step-by-step procedures to restore IT systems.

NIST SP 800-34, Revision 1, states that the five main components of a contingency plan include: Supporting Information, Activation and Notification Phase, Recovery Phase, Reconstitution Phase, and Appendices. "The supporting information and plan appendices provide essential information to ensure a comprehensive plan. The Activation and Notification, Recovery, and Reconstitution Phases address specific actions that the organization should take following a system disruption or emergency."

Failure to establish a thorough contingency plan increases the risk that UHS will not be able to continue business operations in the event of a disaster.

Recommendation 19

We recommend that UHS update its contingency plans in accordance with NIST SP 800-34, Revision 1. Specifically, the documentation should contain detailed step-by-step instructions for recovering IT systems.

Plan Response:

"We feel that [our] Business Continuity plan already takes this into consideration. However we are reviewing your NIST 800-34 to identify and implement relevant information."

OIG Comment:

As part of the audit resolution, UHS should provide OPM's HIO with evidence that its contingency plan has been updated to include critical elements such as points of contact, activation criteria, notifications, recovery, reconstitution, and a BIA.

3. Alternate Recovery Location

UHS does not have an alternate location to recover its computing environment in the event of a disaster. We were told that UHS could potentially recover its IT systems at a contractor facility or at an area medical clinic owned by UHS if the primary location were unavailable. However, UHS has not formally chosen a recovery site or documented the steps necessary to resume operations at such a site.

NIST SP 800-53, Revision 4, states that an organization must establish an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions. Failure to establish an alternate processing site prohibits UHS from continuing business operations in the event of a disaster.

We were told that UHS is in the process of moving its data center from its main facility to an off-site, third-party managed data center. When this transition is complete, the recovery site for IT operations will be the main facility. However, until this transition is complete UHS is still at risk of not being able to continue business operations in the event of a disaster.

Recommendation 20

We recommend that UHS create a plan to recover information system resources at an alternate site if the primary facility is not accessible.

Plan Response:

"We currently have an agreement with our IT consultant group [redacted]. We have tested and they have the resource and capability for information system restore."

OIG Comment:

As part of the audit resolution process, UHS should provide OPM's HIO with evidence that a documented agreement with the IT consultant group [redacted] is in place and a recovery plan has been documented.

This recommendation could also be addressed by providing OPM's HIO with evidence that UHS has migrated its IT environment to the third-party managed data center and a recovery plan has been documented.

4. Data Center Environmental Controls

The current data center that hosts UHS information systems is a dedicated room within the organization’s primary office and medical clinic. The facility provides some environmental controls to protect the availability of systems such as air cooling and alternate power sources. However, the environmental controls could be improved with the implementation of a fire suppression system.

UHS will be moving its primary data center operations to an off-site managed facility in the near future. During the fieldwork phase of the audit, we toured the new data center and observed adequate environmental controls at that facility. After that move takes place, the current server room will be used as a back-up data center and will therefore continue to require sufficient environmental controls to protect the information systems.

NIST SP 800-34, Revision 1, states that “Part of a successful contingency planning policy is making a system resilient to environmental and component-level failures that would otherwise cause system disruptions.”

NIST SP 800-53, Revision 4, requires that “The organization employs and maintains fire suppression and detection devices/systems for the information system ... .”

Failure to provide adequate environmental protection controls in a data center increases the risk that system availability could be negatively impacted by disrupting events.

<u>Recommendation 21</u>

We recommend that UHS improve the environmental controls at the current server room in its primary facility. At a minimum, there should be a fire suppression system to respond to an emergency within that area.

<u>Plan Response:</u>

“We have received one quote for a fire suppression system for our secondary server location at [redacted] Considering the expense we are waiting to review other vendors’ quotes. Expected install of a system will be [redacted]. Our primary Data Center will be off site. A primary data center visit was conducted by OPM team.”

5. Contingency Plan Testing

UHS does not perform contingency plan testing. We were told that UHS has restored data from back-up tapes as a part of a system upgrade. However, UHS does not perform system recovery exercises or tests to determine the effectiveness of the plan and the organizational readiness to execute the plan.

NIST SP 800-34, Revision 1, states that contingency plan testing "is a critical element of a viable contingency capability. Testing enables plan deficiencies to be identified and addressed by validating one or more of the system components and the operability of the plan." NIST SP 800-53, Revision 4, states that the organization must review the contingency plan test results and initiate corrective action.

Failure to test the contingency plan increases the risk that UHS will not be able to recover business operations if unexpected events occur.

Recommendation 22

We recommend that UHS routinely test its contingency plan, document the results, and use the results to update and improve the contingency plan.

Plan Response:

"Critical Servers have been tested and will be tested on a quarterly basis. Documentation will become a standard for updating and improving our contingency plan."

6. Emergency Response Training

UHS does not routinely perform emergency response training. We were told that personnel responsible for responding to disrupting events were part of the plan development process and therefore are aware of the recovery strategies. However, there is no periodic training to reinforce the strategies and activities that personnel will need to perform in an emergency situation.

FISCAM states that "Staff should be trained in and aware of their responsibilities in preventing, mitigating, and responding to emergency situations." FISCAM also states that "information security support staff should receive periodic training in emergency fire, water, and alarm incident procedures, as well as in their responsibilities in starting up and running an alternate data processing site."

Recommendation 23

We recommend that UHS provide periodic training to individuals with emergency response responsibilities.

Plan Response:

"Emergency procedures and business continuity affect mainly the engineering and IT staff. Both of these departments were instrumental in the creation of these procedures."

OIG Comment:

As part of the audit resolution process, UHS should provide OPM's HIO with evidence that UHS conducts emergency response training on a periodic basis and that the results of the training is documented.

7. Backup Data Protection

UHS performs full application and data backups to tape on a daily basis. Once per week, the most recent backup is transported offsite for storage at a commercial storage location. [redacted]. The backup data is also not routinely tested to ensure that the process is successful and the data has not been corrupted.

[redacted]

[redacted]

UHS has informed us that the backup process will change after the primary data center is moved to the off-site managed facility. UHS will begin performing data replication between the two facilities for backup purposes and will no longer use tape backups for any purposes.

Recommendation 24

We recommend that UHS implement [redacted] for backup media as long as it is in use by the organization to store sensitive protected health information.

Plan Response:

"Our current system does not have the capacity to support [redacted]. The backup processes will change after the primary data center [is moved]. We plan to use data replication."

OIG Comment:

As part of the audit resolution process, UHS should provide OPM's HIO with evidence that backup data is being replicated in a secure manner or evidence that the system has been upgraded to support [redacted].

F. Application Controls

The following sections detail our review of the applications and business processes supporting UHS's processing of federal data.

1. Application Configuration Management

UHS has adequate controls regarding application configuration management.

We evaluated the policies and procedures governing application development and change control of UHS's claims processing systems.

UHS does not develop or directly make changes to the claims application software. All change requests are submitted to third-party vendors for development and implementation. Software changes received from vendors are tested in a separate environment prior to implementation into production systems.

Nothing came to our attention to indicate that UHS has not implemented adequate controls related to the application configuration management process.

2. Member Encounters and Claims Processing

We evaluated the input, processing, and output controls associated with UHS's electronic transactions related to member encounters and claims adjudication. We observed UHS's procedures to ensure:

- Sufficient input, processing, and output controls over the member encounter and claims adjudication process;
- Encounters and claims are monitored as they are processed through the systems with real time tracking of the system's performance; and
- Claims scheduled for payment are actually paid.

During our walkthrough of UHS's claims process we observed unsecured claims containing protected health information (PHI) in the claims processing area. We were told that after paper claims have been input into the claims processing system the forms are stored in an unlocked file cabinet.

Storing claims in an unsecure manner increases the risk of unintended disclosure of PHI.

Recommendation 25

We recommend that UHS store claims in a secure manner.

Plan Response:

"Claims paper documents have been secured and copies on network are restricted."

OIG Comment:

As part of the audit resolution process, UHS should provide OPM's HIO with evidence that claims are stored in a secure manner.

3. Enrollment

We evaluated UHS's procedures for managing its database of member enrollment data. Enrollment information is received electronically or in paper format and entered into the claims processing system. All enrollment transactions are fully audited to ensure information is entered accurately. We do not have any concerns regarding UHS's enrollment policies and procedures.

4. Debarment

UHS has adequate procedures for updating its claims system with debarred provider information. UHS downloads the OPM OIG debarment list every month and then performs a manual search for matches in the UHS provider database. Any debarred providers that appear in UHS’s provider database are deactivated to prevent claims submitted by that provider from being inappropriately paid during the claims adjudication process. Nothing came to our attention to indicate that UHS has not implemented adequate controls over the debarment process.

IV. MAJOR CONTRIBUTORS TO THIS REPORT

Information Systems Audit Group

[redacted], Auditor-In-Charge

[redacted], Lead IT Auditor

[redacted], IT Auditor

[redacted], IT Auditor

[redacted], Group Chief

APPENDIX

Draft Audit Report Response Document
Report Number 1C-76-00-15-021
Union Health Service, Inc
November 2nd, 2015

Recommendation 1

After review we agree that a more formal risk assessment process should be implemented, along with formal documentation and a periodic review of the risk assessment. See Risk Assessment Policy document attached.

Recommendation 2&3

Network and EMR passwords have been implemented to meet a more stringent authentication requirement. See attached ID's and Password Policy.

Recommendation 4

Privileged user authentication will be evaluated for implementation next year. Consideration on network impact, budget and workflow will be paramount in the decision factor.

Recommendation 5&6

We researched and tested [redacted] active directory monitoring tool. This program provides significant logs that allow users to be monitored in relation to access to our systems. This software has Domain server Sept 30th, 2015 been installed and is fully functional on all servers.

Recommendation 7

We have implemented [redacted] for our server room access. See attached……..Access control system Server Room

Recommendation 8

We do agree to segregate our network with sub networks. Because of the cost and infrastructure impact we have scheduled this project Implementation for [redacted].

Recommendation 9

We have implemented [redacted] monitoring tool. See [redacted] information doc.

Recommendation 10

We are reviewing your suggested article and will continue implement suggested procedures that fit our infrastructure. See: Breach Investigation and Notification Policy. See: Union Health IT Disaster Recovery Plan 2015 (Includes responsible staff and roles)

Recommendation 11

IT network support staff will *p*erform a vulnerability scan every 6 months. Document and remediate all critical vulnerabilities. If there is no apparent fix; propose a procedure using firewalls and limited access plus constant scanning. See: Infrastructure Vulnerability Policy attached.

Recommendation 12&13

We have removed all non-current and non-supported software from servers. We check all software monthly for critical patches and upgrades. After review appropriate and critical software See: IT Risk Assessment Policy

Recommendation 14

We have taken action to remediate the specific technical weakness outlined by applying all patches and hotfixes required on servers. We have also secured our internet and intranet servers by applying [redacted]. See: Infrastructure Vulnerability Policy

Recommendation 15

See baseline server configuration documentation

Recommendation 16

To assure that our network servers' security configurations are in compliance, we will check all servers quarterly.

Recommendation 17

Standard application operating Patches are always tested in test environments for critical application. Before applying patches to production a snap shot is taken. Snap shots are used for application restore in case of an issue. Other patches are applied based on industry standards

Recommendation 18&19

We feel that Business Continuity plan already takes this into consideration. However we are reviewing your NIST 800-34 to identify and implement relevant information.

Recommendation 20

We currently have an agreement with our IT consultant group [redacted]. We have tested and they have the resource and capability for information system restore.

Recommendation 21

We have received one quote for a fire suppression system for our secondary server location at [redacted]. Considering the expense we are waiting to review other vendors' quotes. Expected install of a system will be [redacted]. Our primary Data Center will be off site. A primary data center visit was conducted by OPM team.

Recommendation 22

Critical Servers have been tested and will be tested on a quarterly basis. Documentation will become a standard for updating and improving our contingency plan.

Recommendation 23

Emergency procedures and business continuity affect mainly the engineering and IT staff. Both of these departments were instrumental in the creation of these procedures

R*ecommendation 24*

Our current system does not have the capacity to support [redacted]. The backup processes will change after the primary data center. We plan to use data replication.

Recommendation 25

Claims paper documents have been secured and copies on network are restricted.

Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in Government concerns everyone: Office of the Inspector General staff, agency employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to OPM programs and operations. You can report allegations to us in several ways:

By Internet: http://www.opm.gov/our-inspector-general/hotline-to-report-fraud-waste-or-abuse

By Phone:

Toll Free Number:	(877) 499-7295
Washington Metro Area:	(202) 606-2423

By Mail:

Office of the Inspector General
U.S. Office of Personnel Management
1900 E Street, NW
Room 6400
Washington, DC 20415-1100